Recent results on p-ranks and Smith normal forms of some $2-(v,k,\lambda)$ designs

Qing Xiang

Abstract. We survey recent results on p-ranks and Smith normal forms of some $2-(v,k,\lambda)$ designs. In particular, we give a description of the recent work in [**11**] on the Smith normal forms of the 2-designs arising from projective and affine spaces over $\mathbb{F}_q$.

1. Introduction

A $2-(v,k,\lambda)$ *design* is a pair $(\mathcal{P},\mathcal{B})$ where $\mathcal{P}$ is a v-set and $\mathcal{B}$ is a collection of b subsets of $\mathcal{P}$ (*blocks*), each of size k, such that any 2-subset of $\mathcal{P}$ is contained in exactly λ blocks. Simple counting arguments show that $b=\frac{\lambda v(v-1)}{k(k-1)}$, and the number of blocks containing each element of $\mathcal{P}$ is $\frac{\lambda(v-1)}{k-1}$, which will be denoted by r (called the *replication number* of the design). The *order* of the 2-design, denoted by n, is defined to be $r-\lambda$. A $2-(v,k,\lambda)$ design $(\mathcal{P},\mathcal{B})$ is said to be *simple* if it does not have repeated blocks (i.e., $\mathcal{B}$ is a set). We will only consider simple 2-designs in this paper. A simple $2-(v,k,\lambda)$ design $(\mathcal{P},\mathcal{B})$ is called *symmetric* (or *square*) if $b=v$.

Classical examples of 2-designs arise from projective and affine spaces over finite fields. Let $\mathrm{PG}(m,q)$ be the m-dimensional projective space over the finite field $\mathbb{F}_q$, where q is a prime power, let $\mathrm{AG}(m,q)$ be the m-dimensional affine space over $\mathbb{F}_q$, and let $\begin{bmatrix} m \\ i \end{bmatrix}_q$ denote the number of i-dimensional subspaces of an m-dimensional vector space over $\mathbb{F}_q$. We have the following classical examples of 2-designs.

Example 1.1. Let $m\geq 2$ and $m\geq d\geq 2$ be integers. The points of $\mathrm{PG}(m,q)$ and the $(d-1)$-dimensional subspaces of $\mathrm{PG}(m,q)$ form a 2-design with parameters $v=\begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q=(q^{m+1}-1)/(q-1)$, $k=\begin{bmatrix} d \\ 1 \end{bmatrix}_q=(q^d-1)/(q-1)$, $r=\begin{bmatrix} m \\ d-1 \end{bmatrix}_q$, $\lambda=\begin{bmatrix} m-1 \\ d-2 \end{bmatrix}_q$, and $b=\begin{bmatrix} m+1 \\ d \end{bmatrix}_q$.

1991 *Mathematics Subject Classification.* Primary 05E20, 05B10; Secondary 20G05, 94B05.

Key words and phrases. code, design, difference set, invariant factor, Jacobi sum, module, p-rank, Smith normal form, unital.

The author was supported in part by NSA grant MDA904-01-1-0036.

Example 1.2. Let $m \geq 2$ and $m-1 \geq d \geq 1$ be integers. The points of $\mathrm{AG}(m,q)$ and the d-flats of $\mathrm{AG}(m,q)$ form a 2-design with parameters $v = q^m$, $k = q^d$, $r = \begin{bmatrix} m \\ d \end{bmatrix}_q$, $\lambda = \begin{bmatrix} m-1 \\ d-1 \end{bmatrix}_q$, and $b = q^{m-d} \begin{bmatrix} m \\ d \end{bmatrix}_q$. Here the d-flats of $\mathrm{AG}(m,q)$ are the cosets of d-dimensional subspaces of the underlying m-dimensional vector space over $\mathbb{F}_q$.

In this paper, we will consider the 2-designs in the above examples in detail. Other designs considered are difference sets and unitals, which will be defined in the coming sections.

Given two $2-(v,k,\lambda)$ designs $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$, we say that $\mathcal{D}_1$ and $\mathcal{D}_2$ are *isomorphic* if there exists a bijection $\phi : \mathcal{P}_1 \to \mathcal{P}_2$ such that $\phi(\mathcal{B}_1) = \mathcal{B}_2$ and for all $p \in \mathcal{P}_1$ and $B \in \mathcal{B}_1$, $p \in B$ if and only if $\phi(p) \in \phi(B)$. An *automorphism* of a 2-design is an isomorphism of the design with itself. The set of all automorphisms of a 2-design forms a group, *the (full) automorphism group* of the design. An *automorphism group* of a 2-design is any subgroup of the full automorphism group.

Isomorphism of designs can also be defined more algebraically by using incidence matrices of designs, which we define now. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $2-(v,k,\lambda)$ design and label the points as $p_1, p_2, \ldots, p_v$ and the blocks as $B_1, B_2, \ldots, B_b$. An *incidence matrix* of $(\mathcal{P}, \mathcal{B})$ is the matrix $A = (a_{ij})$ whose rows are indexed by the blocks B_i and whose columns are indexed by the points p_j, where the entry a_{ij} is 1 if $p_j \in B_i$, and 0 otherwise. From the definition of 2-designs, we see that the matrix A satisfies

$$A^\top A = (r-\lambda)I + \lambda J, \; AJ = kJ, \tag{1.1}$$

where I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix with all entries equal to 1. Note that the first equation in (1.1) tells us that the rank of A over $\mathbb{Q}$ is v. Now let $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ be two $2-(v,k,\lambda)$ designs, and let A_1 and A_2 be incidence matrices of $\mathcal{D}_1$ and $\mathcal{D}_2$ respectively. Then $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic if and only if there are permutation matrices P and Q such that

$$PA_1Q = A_2, \tag{1.2}$$

that is, the matrices A_1 and A_2 are permutation equivalent.

Next we define codes, p-ranks, and Smith normal forms of 2-designs. Let $\mathcal{D}$ be a $2-(v,k,\lambda)$ design with incidence matrix A. The *p-rank* of $\mathcal{D}$ is defined as the rank of A over a field F of characteristic p, and it will be denoted by $\mathrm{rank}_p(\mathcal{D})$. The F-vector space spanned by the rows of A is called the *(block) code* of $\mathcal{D}$ over F, which is denoted by $C_F(\mathcal{D})$. If $F = \mathbb{F}_q$, where q is a power of p, then we denote the code of $\mathcal{D}$ over $\mathbb{F}_q$ by $C_q(\mathcal{D})$. We proceed to define the Smith normal form of $\mathcal{D}$. Let R be a principal ideal domain. Viewing A as a matrix with entries in R, we can find (see for example, [**12**]) two invertible matrices U and V over R such that

$$UAV = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & d_{v-1} & 0 \\ 0 & & \cdots & 0 & d_v \\ 0 & & \cdots & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} \tag{1.3}$$

with $d_1 | d_2 | \cdots | d_v$. The d_i are unique up to units in R. When $R = \mathbb{Z}$, the d_i are integers, and they are called the *invariant factors of* A; the matrix in the right hand side of (1.3) (now with integer entries) is called the *Smith normal form* (SNF) *of* A. We define the *Smith normal form of* $\mathcal{D}$ to be that of A. Smith normal forms and p-ranks of 2-designs can help distinguish nonisomorphic 2-designs with the same parameters: let $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ be two $2-(v, k, \lambda)$ designs with incidence matrices A_1 and A_2 respectively. From (1.2) we see that if $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic, then A_1 and A_2 have the same Smith normal form over $\mathbb{Z}$; hence $\mathcal{D}_1$ and $\mathcal{D}_2$ have the same Smith normal form, in particular, $\mathrm{rank}_p(\mathcal{D}_1) = \mathrm{rank}_p(\mathcal{D}_2)$ for any prime p. Furthermore Smith normal forms of symmetric designs are used by Lander [**25**] to construct a sequence of p-ary codes which carry information about the designs. Therefore it is interesting to study the codes and Smith normal forms of 2-designs.

We collect some general results on p-ranks and Smith normal forms of 2-designs.

THEOREM 1.3 (Theorem 2.4.1 in [**5**]). *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $2-(v, k, \lambda)$ design with order n. Let p be a prime and let F be a field of characteristic p, where $p \nmid n$. Then*

$$\mathrm{rank}_p(\mathcal{D}) \geq v - 1$$

with equality if and only if $p|k$; in the case of equality we have that $C_F(\mathcal{D}) = (F\mathbf{j})^{\perp}$ and otherwise $C_F(\mathcal{D}) = F^{\mathcal{P}}$. Here $\mathbf{j}$ is the all one row vector of length v.

For primes p dividing n, Klemm [**23**] proved the following result.

THEOREM 1.4 (Klemm). *Let $\mathcal{D}$ be a $2-(v, k, \lambda)$ design with order n and let p be a prime dividing n. Then*

$$\mathrm{rank}_p(\mathcal{D}) \leq \frac{b+1}{2}. \tag{1.4}$$

Moreover, if $p \nmid \lambda$ and $p^2 \nmid n$, then

$$C_p(\mathcal{D})^{\perp} \subseteq C_p(\mathcal{D})$$

and $\mathrm{rank}_p(\mathcal{D}) \geq v/2$.

If the design $\mathcal{D}$ above is symmetric (i.e., $b = v$), then the bound in (1.4) becomes

$$\mathrm{rank}_p(\mathcal{D}) \leq \frac{v+1}{2}.$$

This bound is best possible. For example, any skew Hadamard design with parameters $(4n-1, 2n-1, n-1)$ has p-rank equal to $2n$, where p is any prime divisor of n [**28**]. However, for a 2-design which is not symmetric, b is usually much larger than v, and the bound in (1.4) becomes very weak.

Klemm [**24**] also proved some general results on Smith normal forms of 2-designs. He actually proved his results for what he called semi-block designs, in which the block sizes may not be uniform. Here we restrict our attention to 2-designs only.

Theorem 1.5 (Klemm). *Let $\mathcal{D}$ be a $2-(v,k,\lambda)$ design with order n and let $t=\gcd(n,\lambda)$. Let $d_1,d_2,\ldots,d_v$ be the invariant factors of $\mathcal{D}$, where $d_1|d_2|\cdots|d_v$. Then*

(1) *$d_1=1$, $(d_1d_2\cdots d_i)^2|tn^{i-1}$ for $2\le i\le v-1$, and*
$$(d_1d_2\cdots d_v)^2|(n+\lambda v)n^{v-1}.$$
(2) *$d_v|(rn/t)$, and $d_i|n$ for $2\le i\le v-1$.*
(3) *$p|d_i$ for $(b+1)/2<i\le v$ and every prime p dividing n.*

For symmetric designs, the above theorem can be improved.

Theorem 1.6 (Klemm). *Let $\mathcal{D}$ be a $2-(v,k,\lambda)$ symmetric design with order n and let $t=\gcd(n,\lambda)$. Let $d_1,d_2,\ldots,d_v$ be the invariant factors of $\mathcal{D}$, where $d_1|d_2|\cdots|d_v$. Then*

(1) *$d_1d_2\cdots d_v=kn^{(v-1)/2}$.*
(2) *$d_v=kn/t$.*
(3) *Let p be a prime dividing n and $p\not|\lambda$. For any integer x, let x_p denote the p-part of x. Then $(d_id_{v+2-i})_p=n_p$, for $3\le i\le v-1$.*

The rest of the paper is organized as follows. In Section 2, we consider two families of recently constructed cyclic difference sets with parameters $((3^m-1)/2, 3^{m-1}, 2\cdot 3^{m-2})$. These two families of difference sets have the same 3-ranks. Yet they are shown in [**10**] to be inequivalent by using the numbers of 3's in their SNF. In Section 3, we report the recent work in [**11**] on the SNF of the designs in Example 1.1 and 1.2. In Section 4, we collect some recent results on p-ranks and SNF of unitals. We did not intend to be comprehensive. So there might be some recent results on or related to p-ranks and SNF of 2-designs not mentioned here.

2. The invariant factors of some cyclic difference sets

Let $\mathcal{D}=(\mathcal{P},\mathcal{B})$ be a $2-(v,k,\lambda)$ symmetric design with a sharply transitive automorphism group G. Then we can identify the elements of $\mathcal{P}$ with the elements of G. After this identification, each block of $\mathcal{D}$ is now a k-subset of G. Since G acts sharply transitively on $\mathcal{B}$, we may choose a base block $D\subset G$, all other blocks in $\mathcal{B}$ are simply "translates" $gD=\{gx\mid x\in D\}$ of D, where $g\in G$ and $g\ne 1$. That $\mathcal{D}$ is a symmetric design implies
$$|D\cap gD|=\lambda,$$
for all nonidentity element $g\in G$. That is, every nonidentity element $g\in G$ can be written as xy^{-1}, $x,y\in D$, in λ ways. This leads to the definition of difference sets.

Definition 2.1. Let G be a finite (multiplicative) group of order v. A k-element subset D of G is called a (v,k,λ)-*difference set* in G if the list of "differences" xy^{-1}, $x,y\in D$, $x\ne y$, represents each nonidentity element in G exactly λ times.

In the above, we see that sharply transitive symmetric designs give rise to difference sets. In the other direction, if D is a (v, k, λ)-difference set in a group G, then we can use the elements of G as points, and use the "translates" gD of D, $g \in G$, as blocks, and we obtain a symmetric design $(G, \{gD \mid g \in G\})$ with a sharply transitive automorphism group G. (This design is usually called *the symmetric design developed from* D, and will be denoted by $\mathrm{Dev}(D)$.) Hence difference sets and sharply transitive symmetric designs are the same objects.

We will only consider difference sets in abelian groups. Let D_1 and D_2 be two (v, k, λ)-difference sets in an abelian group G. We say that D_1 and D_2 are *equivalent* if there exists an automorphism σ of G and an element $g \in G$ such that $\sigma(D_1) = D_2 g$. Note that if D_1 and D_2 are equivalent, then $\mathrm{Dev}(D_1)$ and $\mathrm{Dev}(D_2)$ are isomorphic. Therefore one way to distinguish inequivalent difference sets is to show that the symmetric designs developed from them are nonisomorphic. This will be the approach we take in this paper. For this purpose, we define p-ranks, invariant factors, and the Smith normal form of a (v, k, λ)-difference set D to be that of the associated design $\mathrm{Dev}(D)$.

In the study of abelian difference sets, characters play an important role. The following is a basic lemma in this area, see [**38**].

Lemma 2.2. *Let G be an abelian group of order v and let D be a k-subset of G. Then D is a (v, k, λ)-difference set in G if and only if*

$$\chi(D)\overline{\chi(D)} = k - \lambda \tag{2.1}$$

for every nontrivial complex character χ of G. Here $\chi(D)$ stands for $\sum_{d \in D} \chi(d)$.

We will see later that if $\gcd(v, k - \lambda) = 1$, then the computations of p-ranks and invariant factors of a difference set D in an abelian group G depend on our understanding of the algebraic integers $\chi(D)$, where χ runs through the character group of G.

The classical examples of difference sets are the Singer difference sets. They arise from the case $d = m$ in Example 1.1. We state this formally below.

Theorem 2.3. *Let q be a prime power and $m > 1$ an integer. Then the points of $\mathrm{PG}(m, q)$ and the $(m-1)$-dimensional subspaces (hyperplanes) of $\mathrm{PG}(m, q)$ form a symmetric design admitting a cyclic sharply transitive automorphism group. That is, the point-hyperplane design in $\mathrm{PG}(m, q)$ is developed from a cyclic difference sets with parameters*

$$v = \frac{q^{m+1} - 1}{q - 1},\ k = \frac{q^m - 1}{q - 1},\ \lambda = \frac{q^{m-1} - 1}{q - 1}. \tag{2.2}$$

The p-ranks of the Singer difference sets were known from 1960's (see [**41**] for detailed references). The Smith normal forms of the Singer difference sets were worked out in full generality by Sin [**36**], and independently by Liebler [**26**]. Since the result on the SNF of Singer difference sets is a special case of the more general results in Section 3, we will not state their results here.

The parameters in (2.2) or the complementary parameters of (2.2) are called *classical parameters.* It is known that there are many infinite families of cyclic difference sets with classical parameters which are inequivalent to the Singer difference sets. For a survey of results up to 1999. we refer the reader to [**41**]. Most of the examples of cyclic difference sets with classical parameters in that survey [**41**] have even q, where q is as in (2.2). More examples with odd q were discovered recently. Here are two examples where q is a power of 3.

We will use standard notation: $\mathbb{F}_{q^m}$ denotes the finite field with q^m elements, $\mathbb{F}_{q^m}^*$ is the multiplicative group of $\mathbb{F}_{q^m}$, $\mathrm{Tr}_{q^m/q}$ denotes the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, and the map $\rho : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ denotes the natural epimorphism.

Example 2.4. Let $q = 3^e$, $e \geq 1$, let $m = 3k$, k a positive integer, $d = q^{2k} - q^k + 1$, and set

$$R = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q}(x + x^d) = 1\}. \tag{2.3}$$

Then $\rho(R)$ is a $((q^m - 1)/(q - 1), q^{m-1}, q^{m-2}(q - 1))$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$.

This is proved by using the language of sequences with ideal 2-level autocorrelation in [**20**] in the case $q = 3$. See [**10**] for a complete proof of this fact (the paper [**10**] also showed that R is a relative difference set). For convenience, we will call this difference set $\rho(R)$ the HKM difference set.

Example 2.5. Let $m \geq 3$ be an odd integer, let $d = 2 \cdot 3^{(m-1)/2} + 1$, and set

$$R = \{x \in \mathbb{F}_{3^m} \mid \mathrm{Tr}_{3^m/3}(x + x^d) = 1\}. \tag{2.4}$$

Then $\rho(R)$ is a $((3^m - 1)/2, 3^{m-1}, 2 \cdot 3^{m-2})$ difference set in $\mathbb{F}_{3^m}^*/\mathbb{F}_3^*$.

This was conjectured by Lin, and recently proved by Arasu, Dillon and Player [**2**]. For convenience, we will call this difference set $\rho(R)$ the Lin difference set.

In the case $q = 3$, $m = 3k$, $k > 1$, the 3-rank of the HKM difference set is $2m^2 - 2m$. This was shown in [**10**] and [**32**]. One can similarly show that the Lin difference set has 3-rank $2m^2 - 2m$, where $m > 3$ is odd, see [**32**]. Therefore when m is an odd multiple of 3, these two difference sets have the same 3-rank. Hence they can not be distinguished by 3-ranks. It is therefore natural to consider using the SNF of these two families of difference sets to distinguish them. We first state a lemma which is very useful for determining the SNF of (v, k, λ)-difference sets with $\gcd(v, n) = 1$.

Lemma 2.6. *Let G be an abelian group of order v, let p be a prime not dividing v, and let $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\xi_v]$ lying above p , where ξ_v is a complex primitive v^{th} root of unity. Let D be a (v, k, λ) difference set in G, and let α be a positive integer. Then the number of invariant factors of D which are not divisible by p^α is equal to the number of complex characters χ of G such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}^\alpha}$.*

Setting $\alpha = 1$ in Lemma 2.6, we see that the p-rank of D is equal to the number of complex characters χ such that $\chi(D) \not\equiv 0 \pmod{\mathfrak{P}}$. This was proved by MacWilliams and Mann [**29**]. For a full proof of the lemma, see [**10**].

Using Lemma 2.6, Fourier transforms, and Stickelberger's congruence on Gauss sums, we [**10**] computed the number of 3's in the SNF of the Lin and HKM difference sets.

Theorem 2.7. *Let $m > 9$. Then the number of 3's in the Smith normal form of the HKM difference sets with parameters $((3^m - 1)/2, 3^{m-1}, 2 \cdot 3^{m-2})$ is*

$$\frac{2}{3}m^4 - 4m^3 - \frac{28}{3}m^2 + 62m + \epsilon(m) \cdot m.$$

The number of 3's in the Smith normal form of the Lin difference sets when $m > 7$ is

$$\frac{2}{3}m^4 - 4m^3 - \frac{14}{3}m^2 + 39m + \delta(m) \cdot m.$$

The values of $\epsilon(m)$ and $\delta(m)$ are 0 or 1.

Based on numerical evidence, we conjecture that δ and ϵ above are always 1. By direct calculations (i.e., not using Gauss sums), the Smith normal form of the Lin difference set with $m = 9$ is:

$$1^{144}3^{1440}9^{1572}27^{1764}81^{1764}243^{1572}729^{1440}2187^{144}6561^{1},$$

where for example, 3^{1440} means the number of invariant factors of the Lin difference set which are 3 is 1440. The Smith normal form of the HKM difference set with $m = 9$ is:

$$1^{144}3^{1251}9^{1842}27^{1683}81^{1683}243^{1842}729^{1251}2187^{144}6561^{1}.$$

These computations were done by Saunders [**34**].

Since the two "almost" polynomial functions in Theorem 2.7 are never equal when $m > 9$, and since the Smith normal forms of the Lin and HKM difference sets are also different when $m = 9$, we have the following conclusion:

THEOREM 2.8. *Let m be an odd multiple of 3. The Lin and HKM difference sets with parameters $(\frac{3^m-1}{2}, 3^{m-1}, 2\cdot 3^{m-2})$ are inequivalent when $m > 3$, and the associated symmetric designs are nonisomorphic when $m > 3$.*

Therefore we successfully distinguished the HKM and Lin difference sets by using the number of 3's in their SNF. At this point, it is natural to ask whether it is true that two symmetric designs with the same parameters and having the same SNF are necessarily isomorphic. The answer to this question is negative. It is known [**4**] that the Smith normal form of a projective plane of order p^2, p prime, is

$$1^r p^{(p^4+p^2-2r+2)}(p^2)^{(r-2)}((p^2+1)p^2)^1,$$

where the exponents indicate the multiplicities of the invariant factors and r is the p-rank of the plane. (This also follows from Theorem 1.6.) That is, the p-rank of the plane completely determines the Smith normal form of the plane. There are four projective planes of order 9. The desarguesian one has 3-rank 37, while the other three all have 3-rank 41 (cf. [**35**]), so the three non-desarguesian projective planes have the same Smith normal form, yet they are nonisomorphic. However, the answer to the following more restricted question is not known.

PROBLEM 2.9. If two cyclic difference sets with classical parameters have the same Smith normal form, are the associated designs necessarily isomorphic?

3. The invariant factors of the incidence matrices of points and subspaces in PG(m, q) and AG(m, q)

In this section, we describe the recent work in [**11**] on the SNF of the designs in Example 1.1 and 1.2. We will concentrate on the design coming from projective geometry first. The SNF of the design coming from AG(m, q) follows from the results in the projective case.

Let PG(m, q) be the m-dimensional projective space over $\mathbb{F}_q$ and let V be the underlying $(m + 1)$-dimensional vector space over $\mathbb{F}_q$, where $q = p^t$, p is a prime. For any d, $1 \le d \le m$, we will refer to d-dimensional subspaces of V as d-subspaces and denote the set of these subspaces in V as $\mathcal{L}_d$. The set of projective points is then $\mathcal{L}_1$. The pair $(\mathcal{L}_1, \mathcal{L}_d)$, where $d > 1$, with incidence being set inclusion, is the 2-design in Example 1.1. Let A be an incidence matrix of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$.

So A is a $b \times v$ $(0,1)$-matrix, where $b = \begin{bmatrix} m+1 \\ d \end{bmatrix}_q$ and $v = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q$. We will determine the Smith normal form of A. There is a somewhat long history of this problem. We refer the reader to [**11**] for a detailed account.

The following theorem shows that all but one invariant factor of A are p powers.

Theorem 3.1. *Let A be the matrix defined as above. The invariant factors of A are all p-powers except for the v^{th} invariant, which is a p-power times $(q^d - 1)/(q-1)$.*

This was known at least from [**37**]. For a detailed proof, see [**11**]. In view of Theorem 3.1, to determine the SNF of A, it suffices to determine the multiplicity of p^i appearing as an invariant factor of A. It will be convenient to view A as a matrix with entries from a p-adic local ring R (some extension ring of $\mathbb{Z}_p$, the ring of p-adic integers). We will define this ring R and introduce a sequence of R-modules and a sequence of q-ary codes in the following subsection.

3.1. R-modules and q-ary codes.

Let $q = p^t$ and let $K = \mathbb{Q}_p(\xi_{q-1})$ be the unique unramified extension of degree t over $\mathbb{Q}_p$, the field of p-adic numbers, where ξ_{q-1} is a primitive $(q-1)^{\text{th}}$ root of unity in K. Let $R = \mathbb{Z}_p[\xi_{q-1}]$ be the ring of integers in K and let $\mathfrak{p}$ be the unique maximal ideal in R (in fact, $\mathfrak{p} = pR$). Then R is a principal ideal domain, and the reduction of $R \pmod{\mathfrak{p}}$ is $\mathbb{F}_q$. Define $\bar{x}$ to be $x \pmod{\mathfrak{p}}$ for $x \in R$.

We now view the above matrix A as a matrix with entries from R. Define

$$M_i = \{x \in R^{\mathcal{L}_1} \mid Ax^\top \in p^i R^{\mathcal{L}_d}\}, \quad i = 0, 1, ...$$

Here we are thinking of elements of $R^{\mathcal{L}_1}$ as row vectors of length v. Then we have a sequence of nested R-modules

$$R^{\mathcal{L}_1} = M_0 \supseteq M_1 \supseteq \cdots$$

Define $\overline{M}_i = \{(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_v) \in \mathbb{F}_q^{\mathcal{L}_1} \mid (x_1, x_2, \ldots, x_v) \in M_i\}$, for $i = 0, 1, 2, \ldots$. For example,

$$\overline{M}_1 = \{(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_v) \in \mathbb{F}_q^{\mathcal{L}_1} \mid A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_v \end{pmatrix} \in pR^{\mathcal{L}_d}\}. \tag{3.1}$$

That is, $\overline{M}_1$ is the dual code of the q-ary (block) code of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$. We have a sequence of nested q-ary code

$$\mathbb{F}_q^{\mathcal{L}_1} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots$$

This is similar to what Lander did for symmetric designs, see [**25**] and [**27**, p. 399]. Note that if $i > \nu_p(d_v)$, where ν_p is the p-adic valuation and d_v is the v^{th} invariant factor of A, then $\overline{M}_i = \{0\}$. It follows that there exists a smallest index ℓ such that $\overline{M}_\ell = \{0\}$. So we have a finite filtration

$$\mathbb{F}_q^{\mathcal{L}_1} = \overline{M}_0 \supseteq \overline{M}_1 \supseteq \cdots \supseteq \overline{M}_\ell = \{0\}.$$

We have the following easy but important lemma. See [**11**] for its proof.

Lemma 3.2. *For $0 \le i \le \ell - 1$, p^i is an invariant factor of A with multiplicity $\dim_{\mathbb{F}_q}(\overline{M}_i/\overline{M}_{i+1})$.*

In what follows, we will determine $\dim_{\mathbb{F}_q}(\overline{M}_i)$, for each $i \geq 0$. In fact, we will construct an $\mathbb{F}_q$-basis for each $\overline{M}_i$. To this end, we construct a basis of $\mathbb{F}_q^{\mathcal{L}_1}$ first.

3.2. Monomial basis of $\mathbb{F}_q^{\mathcal{L}_l}$ and types of basis monomials. Let $V = \mathbb{F}_q^{m+1}$. Then V has a standard basis $v_0, v_1, \ldots, v_m$, where

$$v_i = (\underbrace{0, 0, \ldots, 0, 1}_{i+1}, 0, \ldots, 0).$$

We regard $\mathbb{F}_q^V$ as the space of functions from V to $\mathbb{F}_q$. Any function $f \in \mathbb{F}_q^V$ can be given as a polynomial function of $m+1$ variables corresponding to the $m+1$ coordinate positions: write the vector $\mathbf{x} \in V$ as

$$\mathbf{x} = (x_0, x_1, \ldots, x_m) = \sum_{i=0}^{m} x_i v_i;$$

then $f = f(x_0, x_1, \ldots, x_m)$. The function x_i is, for example, the linear functional that projects a vector in V onto its i^{th} coordinate in the standard basis.

As a function on V, $x_i^q = x_i$, for each $i = 0, 1, \ldots, m$, so we obtain all the functions via the q^{m+1} monomial functions

$$\{\prod_{i=0}^{m} x_i^{b_i} \mid 0 \leq b_i < q, i = 0, 1, \ldots, m\}. \tag{3.2}$$

Since the characteristic function of $\{0\}$ in V is $\prod_{i=0}^{m}(1 - x_i^{q-1})$, we obtain a basis for $\mathbb{F}_q^{V \setminus \{0\}}$ by excluding $x_0^{q-1} x_1^{q-1} \cdots x_m^{q-1}$ from the set in (3.2) (some authors prefer to exclude $x_0^0 x_1^0 \cdots x_m^0$, see [**17**]).

The functions on $V \setminus \{0\}$ which descend to $\mathcal{L}_1$ are exactly those which are invariant under scalar multiplication by $\mathbb{F}_q^*$. Therefore we obtain a basis $\mathcal{M}$ of $\mathbb{F}_q^{\mathcal{L}_1}$ as follows.

$$\mathcal{M} = \{\prod_{i=0}^{m} x_i^{b_i} \mid 0 \leq b_i < q, \sum_i b_i \equiv 0 \pmod{q-1}, (b_0, b_1, \ldots, b_m) \neq (q-1, q-1, \ldots, q-1)\}.$$

This basis $\mathcal{M}$ will be called the *monomial basis* of $\mathbb{F}_q^{\mathcal{L}_1}$, and its elements are called *basis monomials.*

Next we define the type of a nonconstant basis monomial. Let $\mathcal{H}$ denote the set of t-tuples $(s_0, s_1, \ldots, s_{t-1})$ of integers satisfying (for $0 \leq j \leq t-1$) the following:

$$\begin{aligned} &(1) \quad 1 \leq s_j \leq m, \\ &(2) \quad 0 \leq p s_{j+1} - s_j \leq (p-1)(m+1), \end{aligned} \tag{3.3}$$

with the subscripts read (mod t). The set $\mathcal{H}$ was introduced in [**19**], and used in [**9**] to describe the module structure of $\mathbb{F}_q^{\mathcal{L}_1}$ under the natural action of $\mathrm{GL}(m+1, q)$.

For a nonconstant basis monomial

$$f(x_0, x_1, \ldots, x_m) = x_0^{b_0} \cdots x_m^{b_m},$$

in $\mathcal{M}$, we expand the exponents

$$b_i = a_{i,0} + p a_{i,1} + \cdots + p^{t-1} a_{i,t-1} \quad 0 \leq a_{i,j} \leq p-1$$

and let

$$\lambda_j = a_{0,j} + \cdots + a_{m,j}. \tag{3.4}$$

Because the total degree $\sum_{i=0}^{m} b_i$ is divisible by $q-1$, there is a uniquely defined t-tuple $(s_0, \ldots, s_{t-1}) \in \mathcal{H}$ [**9**] such that

$$\lambda_j = ps_{j+1} - s_j.$$

Explicitly

$$s_j = \frac{1}{q-1} \sum_{i=0}^{m} \big(\sum_{\ell=0}^{j-1} p^{\ell+t-j} a_{i,\ell} + \sum_{\ell=j}^{t-1} p^{\ell-j} a_{i,\ell} \big) \tag{3.5}$$

One way of interpreting the numbers s_j is that the total degree of f^{p^i} is $s_{t-i}(q-1)$, when the exponent of each coordinate x_i is reduced to be no more than $q-1$ by the substitution $x_i^q = x_i$. We will say that f is of *type* $(s_0, s_1, \ldots, s_{t-1})$.

Let c_i be the coefficient of x^i in the expansion of $(\sum_{k=0}^{p-1} x^k)^{m+1}$. Explicitly,

$$c_i = \sum_{j=0}^{\lfloor i/p \rfloor} (-1)^j \binom{m+1}{j} \binom{m+i-jp}{m}.$$

Lemma 3.3. *Let c_i and λ_j be as defined above. The number of basis monomials in $\mathcal{M}$ of type $(s_0, s_1, \ldots, s_{t-1})$ is $\prod_{j=0}^{t-1} c_{\lambda_j}$.*

The proof of this lemma is straightforward, see [**11**]. For $(s_0, s_1, \ldots, s_{t-1}) \in \mathcal{H}$, we will use $c_{(s_0, s_1, \ldots, c_{t-1})}$ to denote the number of basis monomials in $\mathcal{M}$. The above lemma gives a formula for $c_{(s_0, s_1, \ldots, c_{t-1})}$.

3.3. Modules of the general linear group, Hamada's formula and the SNF of A. Let $G = \mathrm{GL}(m+1, q)$. Then G acts on $\mathcal{L}_1$ and $\mathcal{L}_d$, and G is an automorphism group of the design $(\mathcal{L}_1, \mathcal{L}_d)$. Hence each M_i is an RG-submodule of $R^{\mathcal{L}_1}$ and each $\overline{M}_i$ is an $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$. In [**9**], the submodule lattice of $\mathbb{F}_q^{\mathcal{L}_1}$ is completely determined. We will need the following result which follows easily from the results in [**9**]. To simplify the statement of the theorem, we say that a basis monomial $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ *appears* in a function $f \in \mathbb{F}_q^{\mathcal{L}_1}$ if when we write f as the linear combination of basis monomials, the coefficient of $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ is nonzero.

Theorem 3.4.

(1) *Every $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ has a basis consisting of all basis monomials in the submodule.*
(2) *Let M be any $\mathbb{F}_q G$-submodule of $\mathbb{F}_q^{\mathcal{L}_1}$ and let $f \in \mathbb{F}_q^{\mathcal{L}_1}$. Then $f \in M$ if and only if each monomial appearing in f is in M.*

For the proof of (1), see [**11**]. Part (2) follows from part (1) easily. The following is the main theorem on $\overline{M}_1$. It was proved by Delsarte [**13**] in 1970, and later in [**17**] and [**9**].

Theorem 3.5. *Let $\overline{M}_1$ be defined as above, i.e., $\overline{M}_1$ is the dual code of the q-ary (block) code of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$.*

(1) *For any $f \in \mathbb{F}_q^{\mathcal{L}_1}$, we have $f \in \overline{M}_1$ if and only if every basis monomial appearing in f is in $\overline{M}_1$.*
(2) *Let $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m}$ be a basis monomial of type $(s_0, s_1, \ldots, s_{t-1})$. Then $x_0^{b_0} x_1^{b_1} \cdots x_m^{b_m} \in \overline{M}_1$ if and only if there exists some j, $0 \leq j \leq t-1$, such that $s_j < d$.*

This is what Glynn and Hirschfeld [**17**] called "the main theorem of geometric codes". As a corollary, we have

Corollary 3.6.

(1) The dimension of $\overline{M}_1$ is

$$\dim_{\mathbb{F}_q} \overline{M}_1 = \sum_{\substack{(s_0,s_1,\ldots,s_{t-1})\in\mathcal{H} \\ \exists j, s_j<d}} c_{(s_0,s_1,\ldots,s_{t-1})}.$$

(2) The p-rank of A is

$$\operatorname{rank}_p(A) = 1 + \sum_{\substack{(s_0,s_1,\ldots,s_{t-1})\in\mathcal{H} \\ \forall j, s_j\geq d}} c_{(s_0,s_1,\ldots,s_{t-1})}.$$

The rank formula in part (2) of the above corollary is the so-called Hamada's formula.

Generalizing Theorem 3.5, we proved the following theorem in [**11**].

Theorem 3.7. *Let $\alpha \geq 1$ be an integer, and let $\overline{M}_\alpha$ be defined as above.*

(1) *For any $f \in \mathbb{F}_q^{\mathcal{L}_1}$, we have $f \in \overline{M}_\alpha$ if and only if every basis monomial appearing in f is in $\overline{M}_\alpha$.*
(2) *Let $x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m}$ be a basis monomial of type $(s_0, s_1, \ldots, s_{t-1})$. Then $x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m} \in \overline{M}_\alpha$ if and only if $\sum_{j=0}^{t-1}\max\{0, d-s_j\} \geq \alpha$*

An immediate corollary is

Corollary 3.8. Let $0 \leq \alpha \leq (d-1)t$, and let $h(\alpha, m, d+1)$ be the multiplicity of p^α appearing as an invariant factor of A. Then

$$h(\alpha, m, d+1) = \delta(0,\alpha) + \sum_{\substack{(s_0,s_1,\ldots,s_{t-1})\in\mathcal{H} \\ \sum_j \max\{0,d-s_j\}=\alpha}} c_{(s_0,s_1,\ldots,s_{t-1})},$$

where

$$\delta(0,\alpha) = \begin{cases} 1, & \text{if } \alpha = 0, \\ 0, & \text{otherwise.} \end{cases}$$

We give some indication on how Theorem 3.7 was proved in [**11**]. Of course Part (1) of Theorem 3.7 follows from the more general result in Theorem 3.4. About Part (2) of the theorem, if $\sum_{j=0}^{t-1}\max\{0, d-s_j\} \geq \alpha$, we need to show that there exists a lifting of the monomial $x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m}$ to $R^{\mathcal{L}_1}$ that is in M_α. It turns out that the Teichmüller lifting $T(x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m})$ of $x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m}$ will suit our purpose. Indeed to show that $T(x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m}) \in M_\alpha$, we used a theorem of Wan [**39**] which gives a lower bound on the p-adic valuation of multiplicative character sums. For details, we refer the reader to [**11**]. The other direction of Part (2) of Theorem 3.7 is much more difficult to prove. We need to prove that if $\sum_{j=0}^{t-1}\max\{0, d-s_j\} < \alpha$, then no lifting of $x_0^{b_0}x_1^{b_1}\cdots x_m^{b_m}$ to $R^{\mathcal{L}_1}$ is in M_α. We need to use the action of G on M_α, Jacobi sums, and Stickelberger's theorem on Gauss sums to achieve this. See [**11**] for details.

3.4. The SNF of the 2-design in Example 1.2. Let $\mathrm{AG}(m, q)$ be the m-dimensional affine space over $\mathbb{F}_q$, where $q = p^t$, p is a prime. Let $\mathcal{D}$ be the design in Example 1.2, i.e., the design of the points and d-flats of $\mathrm{AG}(m, q)$. Let A' be an incidence matrix of $\mathcal{D}$. By viewing $\mathrm{AG}(m, q)$ as obtained from $\mathrm{PG}(m, q)$ by deleting a hyperplane, we prove the following theorem in [**11**].

Theorem 3.9. *The invariant factors of A' are p^α, $0 \leq \alpha \leq dt$, with multiplicity $h(\alpha, m, d+1) - h(\alpha, m-1, d+1)$, where $h(\alpha, \cdot, \cdot)$ is defined in Corollary 3.8.*

In closing this section, we mention the following open problem. Adopting the notation introduced at the beginning of this section, we let $A_{d,e}$ be a (0,1)-matrix with rows indexed by elements Y of $\mathcal{L}_d$ and columns indexed by elements Z of $\mathcal{L}_e$, and with the (Y, Z) entry equal to 1 if and only if $Z \subset Y$. Note that $A_{d,1} = A$, an incidence matrix of the 2-design $(\mathcal{L}_1, \mathcal{L}_d)$. We are interested in finding the Smith normal form of $A_{d,e}$ when $e > 1$.

Problem 3.10. Let $e > 1$. What is the p-rank of $A_{d,e}$? And what is the SNF of $A_{d,e}$?

The first question in Problem 3.10 appeared in [**18**], and later in [**7**]. The ℓ-rank of $A_{d,e}$, where $\ell \neq p$ is a prime, is known from [**15**].

4. p-ranks and SNF of unitals

A *unital* is a 2-$(m^3+1, m+1, 1)$ design, where $m \geq 2$. All known unitals with parameters $(m^3+1, m+1, 1)$ have m equal to a prime power, except for one example with $m = 6$ constructed by Mathon [**30**], and independently by Bagchi and Bagchi [**8**]. In this section, we will only consider unitals embedded in $\mathrm{PG}(2, q^2)$, i.e., unitals coming from a set of $q^3 + 1$ points of $\mathrm{PG}(2, q^2)$ which meets every line of $\mathrm{PG}(2, q^2)$ in either 1 or $q + 1$ points. A classical example of such unitals is *the Hermitian unital* $\mathcal{U} = (\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ and $\mathcal{B}$ are the set of absolute points and the set of non-absolute lines of a unitary polarity of $\mathrm{PG}(2, q^2)$ respectively. Note that the order of $\mathcal{U}$ is $q^2 - 1$. By Theorem 1.3, only the codes $C_p(\mathcal{U})$, with $p|(q-1)$ or $p|(q+1)$, are of interest. Furthermore, it was shown in [**31**] that the codes $C_p(\mathcal{U})$, with $p|(q-1)$ but $p \not| (q+1)$, are the full space. So we only need to consider $C_p(\mathcal{U})$ with $p|(q+1)$. It was conjectured by Andriamanalimanana [**1**] (see also [**6**]) that $\mathrm{rank}_p(\mathcal{U}) = (q^2 - q + 1)q$, if p is a prime dividing $q + 1$. The same conjecture also arose in the work of Geck [**16**], in which he established a close connection between $\mathrm{rank}_p(\mathcal{U})$ and certain decomposition numbers of the three dimensional unitary group.

Building upon [**16**], and the recent important work of Okuyama and Waki [**33**] on decomposition numbers of $\mathrm{SU}(3, q^2)$, Hiss [**22**] determined the SNF of $\mathcal{U}$, hence found the p-rank of $\mathcal{U}$ for every prime p.

Theorem 4.1. *The invariant factors of $\mathcal{U}$ are*

$$1^{(q^3-q^2+q)}(q+1)^{(q^2-q+1)},$$

where the exponents indicate the multiplicities of the invariant factors. In particular, $\mathrm{rank}_p(\mathcal{U}) = q^3 - q^2 + q$ *if* $p|(q+1)$.

The Hermitian unital is a special example of a large class of unitals embedded in $\mathrm{PG}(2, q^2)$, called the Buekenhout-Metz unitals. We refer the reader to [**14**] for a survey of results on these unitals. A subclass of the Buekenhout-Metz unitals which received some attention can be defined as follows.

Let q be an odd prime power, let β be a primitive element of $\mathbb{F}_{q^2}$, and for $r \in \mathbb{F}_q$ let $C_r = \{(1, y, \beta y^2 + r) \mid y \in \mathbb{F}_{q^2})\} \cup \{(0, 0, 1)\}$. We define

$$U_\beta = \cup_{r \in \mathbb{F}_q} C_r.$$

Note that each C_r is a conic in $\mathrm{PG}(2, \mathrm{q}^2)$, any two distinct C_r have only one point $P_\infty = (0, 0, 1)$ in common. Hence $|U_\beta| = q^3 + 1$. It can be shown that every line of $\mathrm{PG}(2, q^2)$ meets U_β in either 1 or $q + 1$ points (see [**3**] and [**21**]). One can immediately obtain a unital (design) $\mathcal{U}_\beta$ from U_β. We use the points of U_β as the *points* of $\mathcal{U}_\beta$, and use the intersections of the secant lines with U_β as *blocks* to get a $2-(q^3+1, q+1, 1)$ design $\mathcal{U}_\beta$. Little is known about the codes of this design. As a first step, consider the binary code $C_2(\mathcal{U}_\beta)$ of this design. The following proposition and conjecture are due to Baker and Wantz.

To state the proposition, we use v^S to denote the characteristic vector of a subset S in U_β.

Proposition 4.2 (Baker and Wantz). *The vectors $v^{C_r}, r \in \mathbb{F}_q$, form a linearly independent set of vectors in $C_2(\mathcal{U}_\beta)^\perp$.*

Proof. A binary vector v lies in $C_2(\mathcal{U}_\beta)^\perp$ if and only if each block of the design meets the support of v in an even number of points. If a block of $\mathcal{U}_\beta$ goes through P_∞, then it meets every C_r in 2 points; if a block of $\mathcal{U}_\beta$ does not go through P_∞, then it meets every C_r in either 0 or 2 points. Hence $v^{C_r} \in C_2(\mathcal{U})^\perp$, for every $r \in \mathbb{F}_q$. The q conics C_r have only one point P_∞ in common. Thus, v^{C_r}, $r \in \mathbb{F}_q$, are linearly independent. This completes the proof. □

An immediate corollary is that $\dim C_2(\mathcal{U}_\beta)^\perp \geq q$, hence $\dim C_2(\mathcal{U}_\beta) \leq q^3+1-q$. Baker and Wantz made the following conjecture.

Conjecture 4.3 (Baker and Wantz). *The 2-rank of $\mathcal{U}_\beta$ is $q^3 + 1 - q$.*

Further computations done by Wantz [**40**] seem to suggest that all invariant factors of $\mathcal{U}_\beta$ are 2-powers, except for the last one, which is a 2-power times $q + 1$.

Acknowledgements: This paper was prepared while the author was visiting Caltech in January, 2004. The author would like to thank Rick Wilson for his support.

References

[1] B. R. Andriamanalimanana, Ovals, unitals and codes, Ph. D. thesis, Lehigh University, 1979.

[2] K. T. Arasu, private communication, July, 2001.

[3] R. D. Baker, G. L. Ebert, *Intersection of unitals in the Desarguesian plane*, Cong. Numer. **70** (1990), 87–94.

[4] E. F. Assmus, Jr., *Applications of algebraic coding theory to finite geometric problems*, in "Finite Geometries: Proceedings of a conference in honor of T. G. Ostrom" (eds. N. L. Johnson, M. J. Kallaher, and C. T. Long), Lect. Notes in Pure and Applied Math. 82, (1983), 23–32.

[5] E. F. Assmus, Jr., J. D. Key, Designs and Their Codes, Cambridge University Press, Cambridge (1992).

[6] E. F. Assmus, Jr., J. D. Key, *Designs and Codes: An update*, Des. Codes and Cryptogr. (1999),

[7] B. Bagchi, S. P. Inamdar, *Projective geometric codes*, J. Combin. Theory Ser. A 99 (2002), no. 1, 128–142.

[8] S. Bagchi, B. Bagchi, *Designs from pairs of finite fields: I A cyclic unital $U(6)$ and other regular Steiner 2-designs*, J. Combin. Theory (A) **52** (1989), 51–61.

[9] M. Bardoe and P. Sin, *The permutation modules for* $\mathrm{GL}(n+1,\mathbb{F}_q)$ *acting on* $\mathbb{P}^n(\mathbb{F}_q)$ *and* $\mathbb{F}_q^{n+1}$, J. London Math. Soc. **61** (2000), 58-80.

[10] D. B. Chandler, Q. Xiang, *Cyclic relative difference sets and their p-ranks*, Designs, Codes and Cryptography **30** (2003), 325–343.

[11] D. B. Chandler, P. Sin, Q. Xiang, *The invariant factors of the incidence matrices of points and subspaces in* $\mathrm{PG}(n,q)$ *and* $\mathrm{AG}(n,q)$, submitted.

[12] P. M. Cohn, Algebra, Volume 1. John Wiley and Sons, Chichester, 1974.

[13] P. Delsarte, *On cyclic codes that are invariant under the general linear group*, IEEE Trans. Information Theory IT-**16** (1970), 760–769.

[14] G. L. Ebert, *Hermitian arcs*, Rend. Circ. Mat. Palermo (2) Suppl. No. 51 (1998), 87–105.

[15] A. Frumkin and A. Yakir, *Rank of inclusion matrices and modular representation theory*, Israel J. Math. **71** (1990), 309–320.

[16] M. Geck, *Irreducible Brauer characters of the 3-dimensional special unitary groups in non-defining characteristic*, Comm. Algebra **18** (1990), 563–584.

[17] D. G. Glynn, J. W. P. Hirschfeld, *On the classification of geometric codes by polynomial functions*, Des. Codes and Cryptogr. **6** (1995), 189–204.

[18] C. D. Godsil, *Problems in algebraic combinatorics*, The Electronic Journal of Combinatorics **2** (1995), #F1.

[19] N. Hamada, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes*, Hiroshima Math. J. **3** (1973), 154–226.

[20] T. Helleseth, P. V. Kumar, and H. M. Martinsen, *A new family of ternary sequences with ideal two-level autocorrelation*, Designs, Codes and Cryptogr. **23** (2001), 157–166.

[21] J. W. P. Hirschfeld, T. Sznyi, *Sets in a finite plane with few intersection numbers and a distinguished point*, Disc. Math. **97** (1991), 229–242.

[22] G. Hiss, *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups*, preprint.

[23] M. Klemm, *Über den p-Rang von Inzidenzmatrizen*, J. Combin. Theory (A), **43** (1986), 138–139.

[24] M. Klemm, *Elementarteiler von Indidenzmatrizen symmetrischer blockpläne*, Geom. Dedicata, **21** (1986), 349–356.

[25] E. S. Lander, Symmetric Designs: An Algebraic Approach, London Math. Society Lecture Note Series **74**, Cambridge University Press, 1983.

[26] R. Liebler, personal communication (2002).

[27] J. van Lint, R. M. Wilson, A Course in Combinatorics, second edition, Cambridge University Press, Cambridge, 2001.

[28] T. S. Michael, *The p-ranks of skew Hadamard designs*, J. Combin. Theory (A) **73** (1996), 170–171.

[29] J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set*, Inform. Control **12** (1968), 474–488.

[30] R. Mathon, *Constructions of cyclic 2-designs*, Ann. Disc. Math. **34** (1987), 353–362.

[31] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. Lond. Math. Soc. (3) **41** (1980), 1–20.

[32] J.-S. No, D.-J. Shin, T. Helleseth, *On the p-ranks and characteristic polynomials of cyclic difference sets*, preprint.

[33] T. Okuyama, K. Waki, *Decomposition numbers of* $\mathrm{SU}(3,q^2)$, J. Algebra **255** (2002), 258–270.

[34] B. D. Saunders, personal communication (2001).

[35] H. E. Sachar, *Error-correcting codes associated with finite projective planes*, Ph. D. thesis, Lehigh University, 1973.

[36] P. Sin, *The invariant factors of the incidence matrices of points and hyperplanes in* $P^n(\mathbb{F}_q)$, preprint.

[37] P. Sin, *The elementary divisors of the incidence matrices of points and linear subspaces in* $P^n(\mathbb{F}_p)$, J. Algebra **232** (2000), 76–85.

[38] R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.

[39] D. Wan, *A Chevalley-Warning approach to p-adic estimates of character sums*, Proc. Amer. Math. Soc., **123** (1995), no. 1, 45–54.

[40] K. Wantz, personal communication (2004).

[41] Q. Xiang, *Recent results on difference sets with classical parameters*, proceedings of the NATO ASI "Difference sets, sequences and their correlation properties", A. Pott et al. (eds.), (1999), 419–437.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716
E-mail address: `xiang@math.udel.edu`